# Accelerating the Development of Biometric Standards

Fernando Podio NIST / ITL, CISD (301) 975-2947 fernando. podio@nist.gov Co-Chair, Biometric Consortium





#### Overview

- Existing Biometric Standards
- Legislative accelerants
- Plans for accelerating the development of biometric standards
- INCITS M1 Biometrics Technical Committee
- Biometric standard incubators
- Summary



#### **Biometric Standards**

Organization	Standard	Status
NIST/BC/NSA	Common Biometric Exchange File Format (CBEFF)	Published Jan 2001 as NISTIR 6529 Being augmented by the NIST/BC Biometric WG - INCITS Fast Track candidate
BioAPI Consortium	BioAPI V1.1 ANSI/INCITS 358	Released March 2001 Fast Track as ANSI/INCITS Stand.
X9 (Financial/Banking)	ANSI X9.84	Approved (ANSI) February 2001
Open Group	Human Recognition.Services (HRS) Module of CDSA	Updated to be consistent with BioAPI
ISO/IEC SC17 WG4	ISO/IEC SC17 7816-11 "Personal Verification Through Biometric Methods"	Committee Draft NIST/BC WG Recommends CBEFF compliance
AAMVA	Nat Stand for Driver Lic/ID Card - Includes fingerprint minutiae	AAMVA DL/ID 2000 Approved 2000
INCITS B10	INCITS 327	Draft based on AAMVA DL/ID 2000
NIST	Data format for finger/facial/SMT	ANSI/NIST-ITL-1-2000 Approved 2000

## **Legislative Accelerants**

- Public Law 107-71 Aviation and Transportation Security
  - Focus on new and emerging technologies that may include biometrics
  - Require action: review of biometrics effectiveness in US airports
  - Potential initiatives related to biometrics:
    - Trusted passenger (TSA establish requirements)
    - Pilot licenses with biometrics
- Public Law 107-56 ("The US Patriot Act"): It requires Justice, State and NIST to certify a "technology standard" that can be used to verify the identity of persons applying for a US visa...
- Pending Senate Bill S1749, "Enhanced Border Security and Visa Entry Reform Act of 2001"
  - Advances deadlines for a technology standard to one year from 2 years in the Patriot Act.
  - Sec. 202 Inserts reference to "appropriate biometric standards" after "technology standard".

## Accelerating the Development of Biometric Standards

- In November 26, 2001 the Executive Board of the International Committee for Information Technology Standards (INCITS) formed Technical Committee M1 – Biometrics
  - > www.ncits.org/press/2001/biometrictcpr.htm
- INCITS is accredited by and operates under rules approved by the American National Standards Institute (ANSI)
- M1 web site
  - > www.ncits.org/tc\_home/m1.htm

#### **INCITS TC M1 Biometrics**

- Purpose:
  - Accelerate the deployment of significantly better, open systems standard-based security solutions for purposes such as homeland defense and the prevention of ID theft as well as other government and commercial applications based on personal biometric authentication.
  - Elevate consortia standards to national and international voluntary consensus standards (e.g., BioAPI, CBEFF).
  - Develop application profiles or implementation agreements (e.g., airport security, border crossing, preventing ID theft) as required.

#### **End Goal**

- Formal International Standards
  - Good for business
    - · Global IT markets
  - Good for homeland defense
    - International cooperation
    - Standard-based implementation agreements
- Generic Biometric Standards
  - Necessary to enable interoperability and data interchange between applications and systems

#### **M1 Biometrics - Status**

- · First meeting:
  - > January 16-17, 2002 at Marriott Metro Center (Washington, DC)
  - > 42 organizations
  - > NIST was asked to convene the first meeting.
- M1 Formed Ad Hoc Group on Organization and Strategy, chaired by Fernando Podio.
- Issued three ballots:
  - ➤ M1 endorsement of ANSI/INCITS 358, **BioAPI Specification**, **V1.1**, for international approval via fast track processing within ISO/IEC JTC 1.
  - Requests that the NIST/BC Biometric WG submit the augmented version of CBEFF, NISTIR 6529-A, when completed for INCITS fast track processing (ANSI) and for subsequent international approval via fast track processing within ISO/IEC JTC 1.
  - ➤ Request of **U.S. TAG assignment** of the generic biometric work in ISO/IEC JTC 1.

### **M1 Biometrics - Membership**

AAMVA ANSER

Apple Computer Biometric Foundation

Bioscrypt

**Business Solutions** 

Ciritec Compaq

Datacard Group Fall Hill Associates

Farance Inc.

Griffin Consulting
ID Technology Partners

Infineon Technologies
Iridian Technologies, Inc.

**KPMG** 

LaserCard Ssystems Corp.

Mitretek Systems

Motorola NIST

Niteo Partners-NEC Solutions

**Open Strategies** 

OSS Nokalva Purdue University Q.E.D. Systems SAFLINK

Sagem Morpho SEARCH

**Security Industry Association** 

Sony

Symbol Technologies, Inc. Texas Instruments Transaction Security

Unisys

United Parcel Service US DOD / DISA US DOD/ BMO US DOJ / NIJ & FBI US DOD / NSA US Department of State

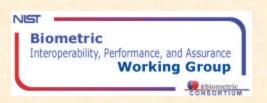
US DOT / Transportation Security

Administration

Visionics Corp.

#### M1 Source for Standards

- Development by M1
- Input from consortia
  - BioAPI Consortium
  - NIST/BC Biometric Interoperability, Performance and Assurance Working Group
  - Others
- It will rely on its members and standards incubators
  - Biometric Consortium
  - BioAPI Consortium
  - NIST
  - IBIA
  - The Biometric Foundation
  - Others



90 organizations
www.nist.gov/bcwg

- Task Groups/Technical Development Teams:
  - > Testing Ad-Hoc Group (Dr. Negin, MNEMONICS) basic testing methodology
  - ➤ Assurance Ad-Hoc Group (Matt King, Booz Allen Hamilton) biometrics assurance issues, review of protection profiles
  - > CBEFF Technical Development Team augmented CBEFF under development (e.g., compliant smart card format, Product ID, nested structure)
  - ➤ Biometric Template Protection & Usage Task Group (Dr. Soutar, BioScrypt) (e.g., risk of re-insertion, template transformations)
  - > Biometric Security Task Force (Catherine Tilton, SAFLINK) (e.g., vulnerability of biometric data to different attacks, non-repudiation)

## Summary

- The development of base generic standards in the last two years set the foundation for achieving system interoperability and biometric data interchange.
- Plans are to leverage from these base generic standards to accelerate the deployment of significantly better, open systems standard-based security solutions for different applications (e.g., DRM, Prevention of ID Theft, Homeland Security, Heath Care, Enterprise Networks, Multi-OS Architectures).
- The end goal is the approval of formal/generic international standards necessary to enable interoperability and data interchange between applications and systems